ARMY RESEARCH LABORATORY

Information Operations Vulnerability/Survivability Assessment (IOVSA): Process Structure

Richard L. zum Brunnen, Christopher D. McDonald, Paul R. Stay,
Michael W. Starks, and Anthony L. Barnes

ARL-TR-2250 June 2000

Army Research Laboratory
Aberdeen Proving Ground, MD 21010-5423

ARL-TR-2250 **June 2000**

Information Operations Vulnerability/Survivability Assessment (IOVSA): Process Structure

Richard L. zum Brunnen, Christopher D. McDonald, Paul R. Stay, Michael W. Starks, and Anthony L. Barnes
Survivability/Lethality Analysis Directorate, ARL

Abstract

The Survivability/Lethality Directorate (SLAD) of the U.S. Army Research Laboratory (ARL) has developed an information operations vulnerability/survivability assessment (IOVSA) process. The objective of the IOVSA process is to establish a systematic approach that permits analysis and evaluation of the survivability of military component level and weapon systems that include information technology (IT) items. The process will apply throughout the life cycle phases of any Department of Defense (DOD) system that collects, stores, transmits, or processes classified and/or sensitive but unclassified (SBU) information, as well as commercial components to DOD systems. The IOVSA process fulfills many of those process activities required by the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) by providing much of the required vulnerability information.

The IOVSA plan for a particular system is a focused plan that has been designed to provide the decision-makers with the necessary information to make informed decisions concerning the susceptibilities and vulnerabilities of the system to information operations (IO) threats. By addressing the IO threats, the system will significantly improve its survivability by planning for both avoiding and withstanding potential problems with IO-based threats. This report discusses the IOVSA process in detail.

Acknowledgments

The authors gratefully acknowledge the useful comments and suggestions provided by Mr. Edward J. Panuska.

INTENTIONALLY LEFT BLANK.

Table of Contents

		Page
	Acknowledgments.	iii
	List of Figures	vii
	List of Tables	vii
1.	**Introduction**	1
1.1	Objective	1
1.2	Scope	1
1.3	Survivability	2
1.4	IOVSA Process	3
1.5	DITSCAP	4
2.	**System Familiarization**	8
2.1	Introduction	8
2.2	The System Familiarization Process	8
2.3	System Description	8
2.4	System Architecture	9
3.	**System Design Analysis**	9
3.1	Introduction	9
3.2	System Functionality Assessment Process	9
3.3	Data Flow Analysis Process	9
4.	**Threat Definition and Susceptibility Assessment**	10
4.1	Introduction	10
4.2	Threat Definition Process	11
4.3	Susceptibility Assessment Characterization Process	12
5.	**Vulnerability Risk Assessment**	13
5.1	Introduction	13
5.2	Analytical Vulnerability Assessment Process	14
5.3	Modeling and Simulation Process	14
5.4	Experimental Vulnerability Assessment Process	22

6.	**Protection Assessment and Recommendations**	23
6.1	Introduction	23
6.2	Process Activities: Protection Assessment and Recommendation Criteria	24
6.3	Sample Assessment Recommendations	24
7.	**Summary**	26
8.	**References**	29
	Appendix: Generic Experimentation Plan for an Information Operations Vulnerability/Survivability Assessment	31
	Glossary	39
	Distribution List	43
	Report Documentation Page	55

List of Figures

Figure		Page
1.	Interaction of the Five Phases of an IOVSA	3
2.	1553b Data Bus	16
3.	OPNET Representation of the 1553b Data Bus	16
4.	OPNET's Representation of a Node	17
5.	Node Module State-Transition Diagram	18
6.	Optional Proto-C Code Within Each Module	18
7.	Model Generated Results	19

List of Tables

Table		Page
1.	The Five Phases of an IOVSA	3
2.	Relationship of IOVSA to DITSCAP Phases, Activities, and Tasks System Familiarization	5

INTENTIONALLY LEFT BLANK.

1. Introduction

1.1 Objective. From 1992 until the present, the Survivability/Lethality Analysis Directorate (SLAD) of the U.S. Army Research Laboratory (ARL) has developed an Information Operations Vulnerability/ Survivability Assessment (IOVSA) process. The objective of the IOVSA process is to establish a systematic approach that permits analysis and evaluation of the survivability of military component level and weapon systems which include information technology (IT) items. The process will apply throughout the life cycle phases of any Department of Defense (DOD) system that collects, stores, transmits, or processes classified and/or sensitive but unclassified (SBU) information. The process will also address commercial systems that are needed to support these DOD systems. Examples include commercial phone, networks, satellites and allied C4I systems. The IOVSA process fulfills many of those process activities required by the DOD information technology security certification and accreditation process (DITSCAP) [1] by providing much of the required vulnerability information.

1.2 Scope. The IOVSA process is designed for implementation on all Defense Department systems and support systems which employ IT and are involved in battlefield operations. This includes all major, nonmajor, commercial off the shelf (COTS), and nondevelopmental items, as well as modifications to systems currently deployed or in production. Most of these systems, if not all, have new DITSCAP requirements. It must be pointed out that by conducting an IOVSA on a system, a Program Executive Officer (PEO) or Project Manager (PM) gets a good distance toward satisfying his/her DITSCAP requirements. Indeed, after conducting an IOVSA, SLAD would be the ideal place to serve as the certification authority in the DITSCAP process.

The process defined in this document establishes a common approach for conducting an assessment flexible enough to be applicable to the broad range of military systems in all branches of the services (U.S. Army, Navy, Marines, and Air Force) at any point in the life cycle of a system. The current process has evolved from the electronic warfare vulnerability assessment (EWVA) process [2] and the SLAD information systems survivability assessment (ISSA) methodology [3].

1.3 Survivability. SLAD is the U.S. Army's primary source of survivability, lethality, and vulnerability (SLV) analysis and evaluation support, adding value over the entire system's life cycle. SLAD's objective is to ensure that soldiers and systems can survive and function on the battlefield. The SLAD mission is to:

- Provide survivability, lethality, and vulnerability analysis and evaluation support over the entire life cycle of major Army systems and to help acquire systems that will survive and/or be highly lethal in all environments against the full spectrum of battlefield threats.

- Provide advice/consultation on SLV issues to Headquarters Department of the Army (HQDA), PEOs/PMs, evaluators, combat developers, battle labs, intelligence activities, and other Department of the Army (DA) and DOD activities.

- Conduct investigations, experiments, simulations, and analyses to quantify SLV of Army and selected foreign weapon systems.

- Provide well-documented, timely technical judgments on complex SLV issues.

- Perform special studies and make recommendations regarding tactics, techniques, or design modifications to reduce vulnerability and enhance survivability and lethality of Army materiel.

- Develop tools, techniques, and methodologies for improving SLV analysis.

From 1992 until the present, SLAD has leveraged its traditional technical strengths in electronic warfare, networking, directed energy, high speed computation, military communications, the employment of Army systems, and systems engineering and analysis in order to develop one of the nation's premier capabilities in information warfare (IW).

1.4 IOVSA Process. An IOVSA may consist of five process activities, as shown in Table 1. The interaction of these steps is shown graphically in Figure 1. However, there are many factors that determine whether all activities actually occur.

Table 1. The Five Phases of an IOVSA

Phase No.	Phase Title
1	System Familiarization
2	System Design Analysis
3	Threat Definition and Susceptibility Assessment
4	Vulnerability Risk Assessment
5	Protection Assessment and Recommendations

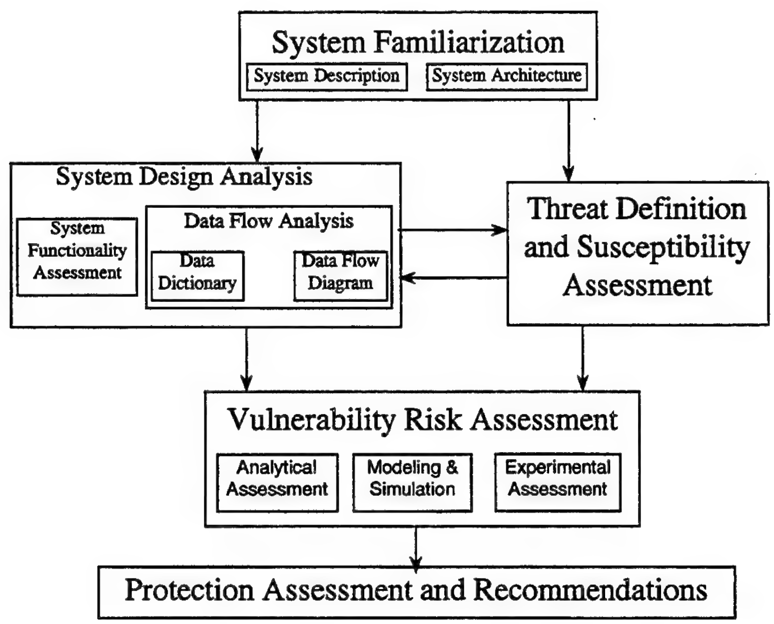

Figure 1. Interaction of the Five Phases of an IOVSA.

For fielded, mature systems with few or no hardware and/or software updates, a detailed system familiarization and system design analysis processes may not be necessary. The system familiarization and system design analysis processes need only be done to the level of detail so that the information operations (IO) analyst gains the necessary knowledge and data to understand the system's mission-critical resources, both hardware and software. The level of

detail to which the system familiarization and system design analysis are done are system dependent. Similarly, the modeling and simulation process may be impractical for all IT systems given the current capabilities of existing force-on-force models to incorporate IO considerations [4].

1.5 DITSCAP. The DITSCAP establishes a standard process, set of activities, general task descriptions, and a management structure to certify and accredit systems that will maintain the security posture of the Defense Information Infrastructure (DII). The DITSCAP focuses on protecting the DII by presenting an infrastructure-centric approach for certification and accreditation (C&A). The DITSCAP is designed to be adaptable to any type of IT and any computing environment and mission. The process should be adapted to include existing system certifications and evaluated products. The IOVSA process fulfills phases I, II, and III of the DITSCAP methodology. Table 2 maps the steps of IOVSA to particular DITSCAP process activities.

The DITSCAP is designed to certify that the system meets accreditation requirements and that the system will continue to maintain the accredited security posture throughout the system's life cycle. The users of the system will align the process with the program strategy and integrate process activities into the system life cycle. While DITSCAP maps to any system life cycle process, its four phases are independent of the life cycle strategy.

The key to the DITSCAP is the agreement between the system program manager, the DAA, the Certification Agent (CA), and the user representative. These managers (or "players" per the DITSCAP CD-ROM) resolve critical schedule, budget, security, functionality, and performance issues. This agreement is documented in the system security authorization agreement (SSAA) that is used to guide and document the results of the C&A. The objective is to use the SSAA to establish a binding agreement on the level of security required before the system development begins or changes to a system are made [5].

Table 2. Relationship of IOVSA to DITSCAP Phases, Activities, and Tasks System Familiarization

DITSCAP Phase	DITSCAP Activities	DITSCAP Task	SLAD IOVSA Steps
phase I, definition	document mission need	determine and document mission functions	1.A and B
	conduct registration	register the system - inform the DAA and the user representative that a system will require C&A support	
		prepare mission description and system identification	1.A
		prepare environment and threat description	3
		prepare system architecture description	1.B
		determine the ITSEC class	
		determine the system security requirements	1
		identify organizations that will support the C&A	
		tailor the DITSCAP tasks, determine the C&A scope, level-of-effort, and prepare the DITSCAP plan	
		develop the draft SSAA	
	perform negotiation	review the draft SSAA	
		conduct the CRR	
		approve the SSAA	
	prepare the SSAA		
phase II, verification	refine the SSAA		
	support system development activities		
	perform certification analysis	system architecture analysis	2.A

Table 2. Relationship of IOVSA to DITSCAP Phases, Activities, and Tasks System Familiarization (continued)

DITSCAP Phase	DITSCAP Activities	DITSCAP Task	SLAD IOVSA Steps
		software design analysis	2.A and 2.B
		network connection rule compliance analysis	4.A and 4.C
		integrity of integrated products analysis	1 – 4
		life cycle management analysis	1 and 2
		vulnerability assessment analysis	4.A, B, and C
	assess analysis results against SSAA requirements		
phase III, validation	refine the SSAA		
	certification evaluation of the integrated system	ST&E	4.A and 4.C
		penetration testing	4.C
		TEMPEST and red-black verification	
		validation of COMSEC compliance	
		system management analysis	
		contingency plan evaluation	4.A and 4.B
		risk-based management review	4.C
	develop recommendation to the DAA	CA's recommendation	5
	DAA accreditation.		
phase IV, post accreditation	maintenance of the SSAA	review the SSAA	
		obtain approval of changes	
		document changes	
	system operation	system maintenance	
		system security management	
		contingency planning	

Table 2. Relationship of IOVSA to DITSCAP Phases, Activities, and Tasks System Familiarization (continued)

DITSCAP Phase	DITSCAP Activities	DITSCAP Task	SLAD IOVSA Steps
	change management	support system configuration management	
		risk-based management review	
	compliance validation	review the SSAA	
		physical security analysis	
		procedural analysis	
		risk-based management review	

2. System Familiarization

2.1 Introduction. The IOVSA process begins with the accumulation of all available information related to the IT system. Related information includes specific technical data, performance requirements, environment description, program definition, planning information, IO strategies, and operational requirements to address survivability. During the research portion of the system familiarization process, the analyst will identify information to be used in subsequent steps of the IOVSA process.

2.2 The System Familiarization Process. The system familiarization process will encompass a review of system documentation, as well as discussions with the PEO or the PM office and its contractors. The purpose is to gain knowledge or data concerning the systems' mission-critical resources, both hardware and software. System documentation, including the operational requirements document (ORD), test and evaluation master plan (TEMP), prime item development specification (PIDS), and software requirement specifications (SRS) will be reviewed. The process has two components: system description and system architecture.

2.3 System Description. Complete understanding of the system is essential to the IOVSA. Obtaining system parameter information requires participation of other agencies and individuals outside of SLAD, so identification of key players mirrors phase I in the DITSCAP methodology. These elements are critical for system description:

(a) system mission,

(b) system requirements,

(c) system specifications,

(d) information assurance (IA) requirements,

(e) data access policies, and

(f) physical characteristics.

2.4 System Architecture. The system architectural description is a high-level overview of the types of hardware, software, firmware, and associated interfaces envisioned for the system. This description should contain an overview of the internal system structure to include the anticipated hardware configuration, application software, software routines, operating systems, remote devices, communications processors, network, and remote interfaces.

3. System Design Analysis

3.1 Introduction. There are two components in the process: a system functionality assessment and a data flow analysis. The first component maps to those tasks involved in the registration process activity in phase I of the DITSCAP. The second component addresses survivability concerns not currently within the DITSCAP process, but which are essential for IO and IA on the battlefield.

3.2 System Functionality Assessment Process. The objective of the functionality assessment is to determine if the system can achieve its specific requirements. Analysis of system requirements and specifications against the system description and architecture permits determination of whether the designed system meets the intended functionality.

3.3 Data Flow Analysis Process. The data flow analysis will formulate the detailed program specifications for an information flow model (IFM) of the system under analysis. These factors will determine specifications for hardware, software, operating systems, protocols, topology, and interconnections between both internal subsystems and external communications. The IFM will provide some initial analytical measure of performance of the system for different configurations and scenarios.

The analysis will be documented in a data flow diagram. The documentation will include data dictionary and transform descriptions. The data dictionary documents each of the interface flows and data stores on any data flow diagram. The transform descriptions document the internals of the data flow diagram processes in a rigorous fashion (usually through the use of structured English, decision tables, and decision trees) [6].

4. Threat Definition and Susceptibility Assessment

4.1 Introduction. The objective of this activity is to identify the threats and susceptibilities of a system. The threats and susceptibilities defined in this part of the analysis will be used to define the vulnerabilities of the system in the vulnerability risk assessment portion of the process. Any system is susceptible to some extent, with the range of susceptibility extending from simple degradation to complete physical destruction. The fact that any system is susceptible does not mean it is vulnerable in the performance of its mission. Threat definition plays the critical role of determining which susceptibilities can actually result in system vulnerabilities. SLAD uses a wide array of both intelligence and technical sources to determine a realistic threat to IT systems. Only threats to which the system component(s) are determined to be susceptible need to be considered in further vulnerability assessments. Together both the threat definition and susceptibility assessment form this important section of the overall IOVSA process.

Susceptibilities are characteristics of a system that a threat might exploit to cause vulnerability. Vulnerabilities affect mission performance and survivability. The entire IOVSA methodology seeks to provide recommendations to eliminate and/or mitigate vulnerabilities to enhance overall survivability.

This step of the IOVSA process provides the basis for performing the vulnerability assessment analysis required by the certification analysis process activity in phase II of the DITSCAP, and for conducting the testing required by the certification evaluation process activity in phase III of the DITSCAP.

4.2 Threat Definition Process. Historically, DOD and the U.S. Army have defined specific classes of threats for IT components of systems including:

(a) compromise or exploitation of information,

(b) corruption of information with loss of data integrity,

(c) destruction or modification of information,

(d) denial or interruption of service, and

(e) physical destruction.

Some of the specific threat mechanisms that are considered within the above threat classes include:

(a) unauthorized user,

(b) insider,

(c) malicious software,

(d) signal intelligence (SIGINT),

(e) radiation intelligence (RINT),

(f) electronic attack,

(g) conventional weapons,

(h) nuclear electromagnetic pulse (EMP),

(i) directed energy weapons (DEW),

(j) nonnuclear EMP,

(k) obscurants,

(l) biological/chemical, and

(m) Other (theft, human error).

Validated threat documents, which relate these classes and mechanisms to individual IT systems, are oftentimes either unavailable or unreliable. This IOVSA process attempts to identify relevant threats, as well as their likelihood of occurrence. In the past, SLAD has worked with the intelligence community, computer emergency response teams (CERT), and the research community to assure that the most current and valid threats to IT systems are considered in the IOVSA.

4.3 Susceptibility Assessment Characterization Process. Known susceptibilities of a specific system are gathered in the susceptibility assessment. Both system components and the overall system are considered in the process. Due to the technical nature of susceptibilities, a large number of sources are used in the generation of the susceptibility list for the system. Some of the sources include:

(a) open source publications,

(b) past tests on systems,

(c) other organizations such as NSA, DIA, and DOE,

(d) hacker databases,

(e) system developers databases,

(f) FBI (National Protection Center) database,

(g) system configuration parameters,

(h) network connectivity information

(i) computer emergency response teams (CERTs), and

(j) IO laboratories such as SLAD, ARL, and Defense Advanced Research Projects Agency (DARPA).

The susceptibility list will then be used in the next step in the process (vulnerability risk assessment) to aid in determining the system's vulnerabilities. The output of this phase will also be applied during the modeling effort.

5. Vulnerability Risk Assessment

5.1 Introduction. The objective of this phase is to identify and confirm vulnerabilities which will impact on the mission of the IT system. Vulnerabilities are the intersection of the sets of susceptibilities and threats. As part of the risk assessment, SLAD takes the list of all system susceptibilities generated in the susceptibility assessment and compares it with the list of threats. If a susceptibility exists that can be exploited, then it becomes a vulnerability. This process reduces the size and therefore the cost of protecting the system since the list of vulnerabilities is always smaller than the list of susceptibilities. There are three components in this phase: analytical vulnerability assessment, modeling and simulation, and experimental vulnerability

assessment. This IOVSA phase provides much of the necessary information required by the certification evaluation process in phases II and III of the DITSCAP.

5.2 Analytical Vulnerability Assessment Process. After the system familiarization and design analysis have been completed and the threat definition and susceptibility assessment have been made, the analyst may be in a position to draw some conclusions concerning the vulnerability of the system. For example:

(a) Within system C if protocol X is used to send a particular packet of size E bits from component A to component B, and

(b) if the packet receive buffer in component B is of size D bits, and

(c) if D (the buffer size in bits) is smaller than E (the packet length in bits) or $D < E$,

(d) then the resulting event (in the case of this example, buffer overflow) is predictable.

An experienced analyst can then predict the result of this, the likelihood of this event, and the degree to which it could possibly affect the ability of the system to complete its mission. This assessment is based on previous experimental results and includes no actual experimentation on the system. An analytical vulnerability assessment lets us leverage accumulated knowledge regarding previously identified system vulnerabilities for the purpose of assessing analogous vulnerabilities in the system under consideration. The output from the analytical vulnerability assessment process forms the foundation for the analytical assessment process.

5.3 Modeling and Simulation Process. The goal of the IOVSA modeling and simulation process is to build a simulation of the system in which the known susceptibilities and vulnerabilities are portrayed as close to the physical system as reasonably possible. All of the previous processes of the IOVSA, as shown in Figure 1 in section 1.4, provide essential inputs to the modeling and simulation process. The system familiarization provides both a description of

the system and the architectural details of the system and of the individual components. The system design analysis provides information concerning the functionality of the system and of its components. The data flow analysis provides information on the data entering and leaving the system; the internal flow of data within and between its components is also supplied. The threat definition provides information on the threats that may have an impact on the system or any of its components. The susceptibility assessment provides information on the known susceptibilities that are specific to the system or to any of its components. The vulnerability risk assessment provides information from two perspectives, analytical and experimental, concerning the system and its individual components. All of this information is required if the modeling and simulation is to accurately represent the system and its components.

For the purposes of discussion, a ground platform is used in the following example. This modeling approach can be applied to any system or system of systems; it is primarily a matter of scale.

Figure 2 shows the layout of the primary nodes connected to the 1553b data bus within a ground platform. The specifics about the system and the layout of its components are provided by the system familiarization. This type of data bus configuration is fairly standard across the "digital" ground fleet. What is not shown on this figure is the connection from other internal system components into the data bus nodes. For example, the radios (Single Channel Ground Airborne Radio System [SINCGARS] and Enhanced Position Location Reporting System [EPLRS]) do not appear. There are many components that are connected to these nodes through various means (e.g., serial connections [RS-170, RS-232, RS-422/423, etc.], small computer system interface [SCSI] connections, personal computer module card interface adapter [PCMIA] connections, etc.). One of the other items that is missing from the diagram in Figure 2 is the utility bus; this bus controls the power feeds to the components internal to the platform.

SLAD's current information flow modeling and simulation efforts use the optimized network engineering tools (OPNET) Modeler simulation environment developed by Mil 3 Corporation of Washington, DC. When created in the OPNET environment, the 1553b data bus model appeared (shown in Figure 3). This model, as with any others created in OPNET, is object oriented and

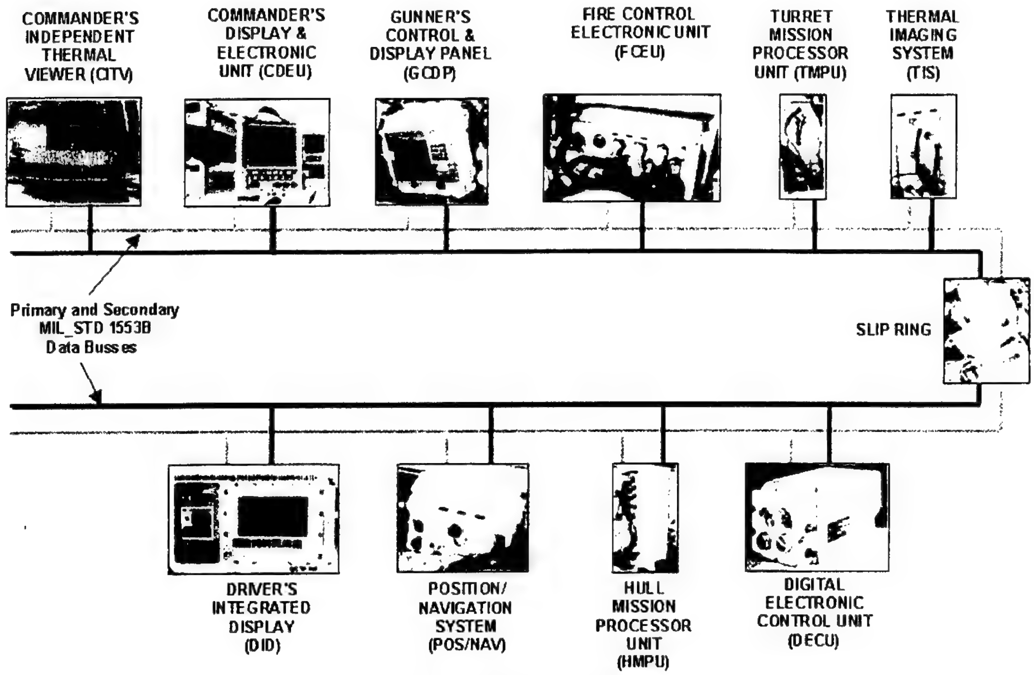

Figure 2. 1553b Data Bus.

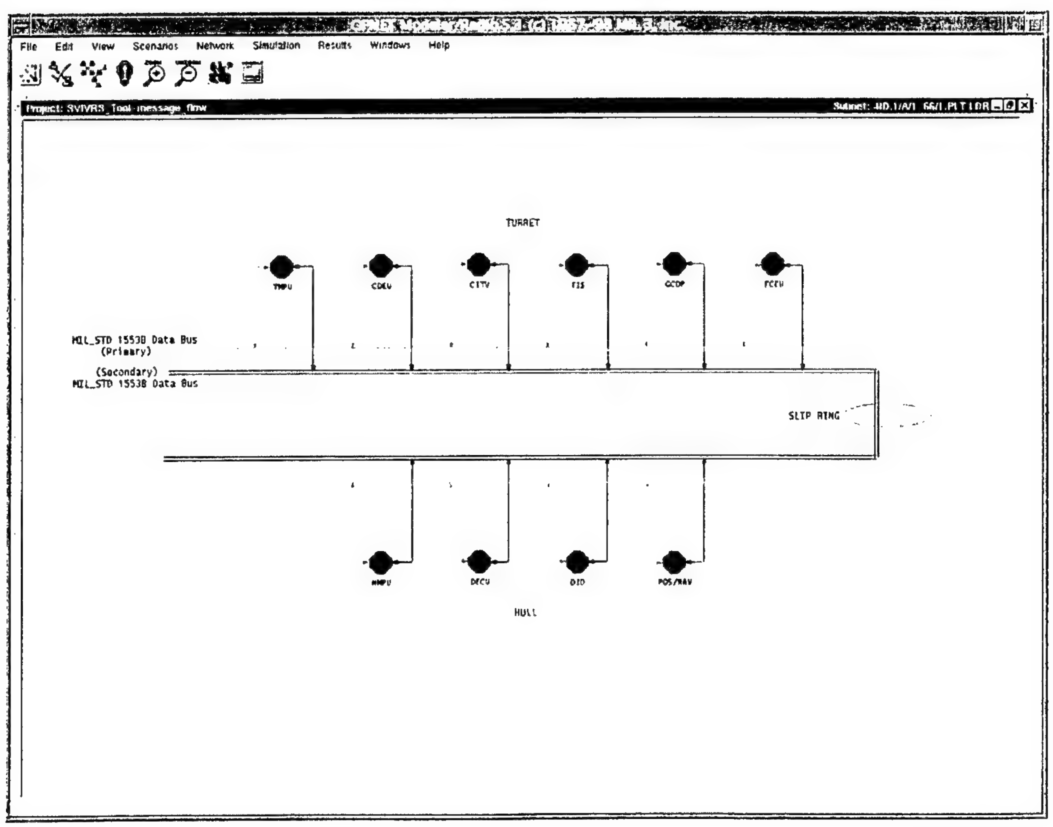

Figure 3. OPNET Representation of the 1553b Data Bus.

modular in design. This model can be reconfigured to accept any number of node and data buses. There are many user definable parameters within the model, such as bus data rate and bit error rate. As with most models built parameters with the model, such as bus data rate and bit error rate. As with models built in the OPNET environment, the wiring of the bus model is a simple "drag and drop"procedure. Most standard types of interface connection are predefined in OPNET and it is fairly easy to construct the architecture for the desired model. The blue nodes in Figure 3 correspond to those pictured in Figure 2.

Figure 4 shows the way that OPNET represents a node from Figure 3, the wiring diagram. Nodes are comprised of modules that control packet flow and statistic collection. Each node in Figure 3 has an underlying set of modules similar to those shown in Figure 4; this underlying set of modules are user configurable and each node can be designed to address specific purposes.

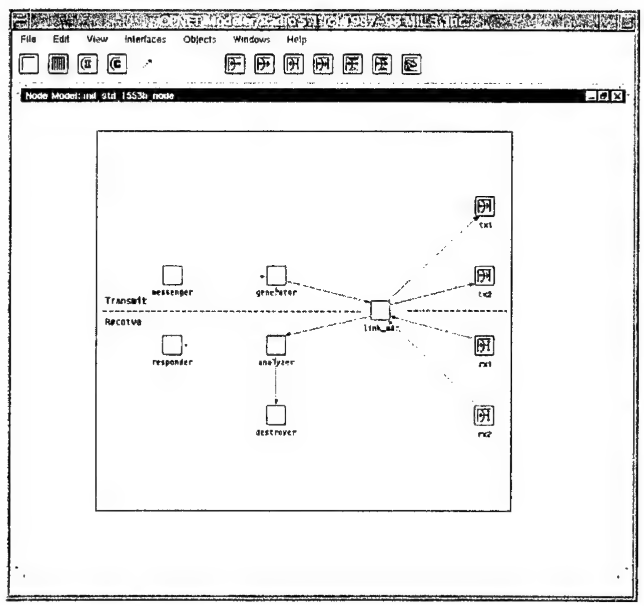

Figure 4. OPNET's Representation of a Node.

For each of the modules in Figure 4, there is a process model that defines the behavior of the module through the use of a state-transition diagram—an example is shown in Figure 5.

Each state of the state-transition diagram can contain a proto-C code that further defines the module's behavior. It is in this proto-C code that the behavior of a module to the specific threats is incorporated. An example of the proto-C code is shown in Figure 6.

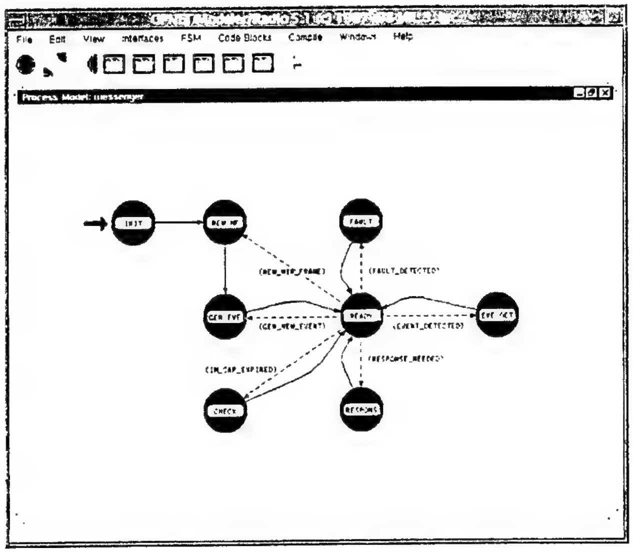

Figure 5. Node Module State-Transition Diagram.

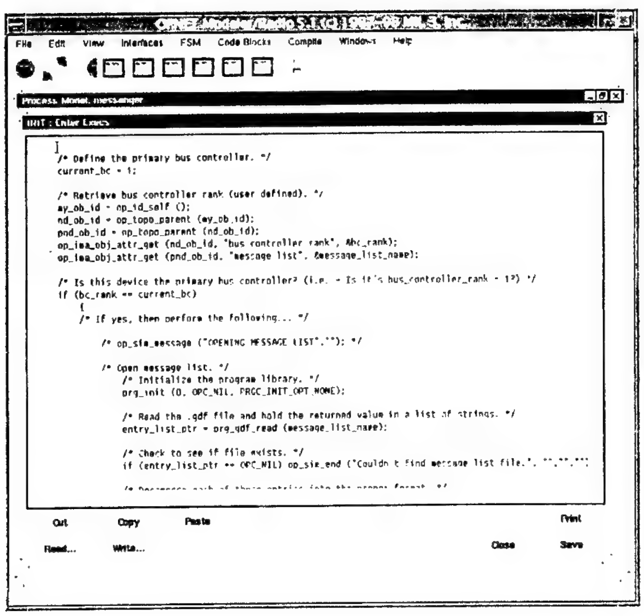

Figure 6. Optional Proto-C Code Within Each Module.

The sequence of Figures 2–6 shows how SLAD is addressing information flow modeling and simulation within an individual battlefield platform. This is a highly detailed approach that involves modeling the threat situations in the modules of the state-transition diagram. For example, in the case of the buffer overflow problem that was presented in section 5.2, the analytical vulnerability assessment process, the cause and effect of this situation has to be understood in enough detail that a programmer can model the situation using proto-C.

Figure 7 presents data bus utilization as a function of time as an example of how one of the collected statistics generated by one run of the model might be presented. The user controls how these collected statistics are displayed and can choose from any number of combinations. These results can be collected over any number of simulations in order to monitor changes in output resulting from changes in input.

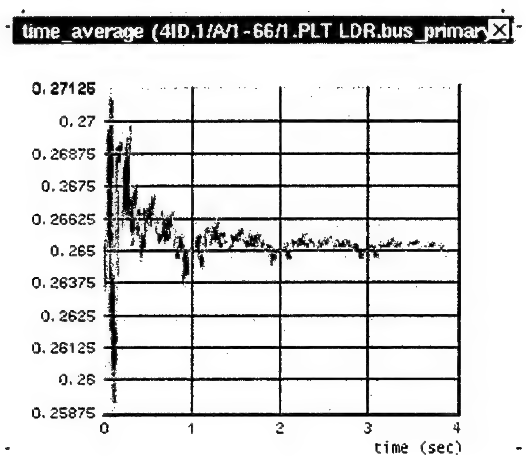

Figure 7. Model Generated Results.

Once the basic OPNET representation of the model is created, as in Figure 3, the complex tasks of configuring the model parameters and loading the desired initial data sets begins. In a highly detailed configuration of the model, the contents of the messages, which travel across the data bus, are of concern. As the scope of the modeling effort changes by moving up the battlefield hierarchy from a battlefield platform to a small group of networked battlefield platforms and then on to a large network made up of multiple networks (systems of systems), the

results generated by the model change. The change of focus is primarily the result of the types of questions being addressed. Across the spectrum of the military component level and on to weapon systems, the purposes and the resolution of the investigations vary. SLAD has broken this spectrum down as follows:

(a) battlefield platform [i.e., Longbow Apache AH64-D, Abrams M1A2 SEP, Bradley M2A3, tactical operations centers (TOC), etc.],

(b) networked battlefield platforms [i.e., force XXI battle command brigade-and-below (FBCB2), maneuver control system (MCS), all source analysis system (ASAS), etc.], and

(c) system-of-systems [i.e., tactical internet (TI), military information infrastructure (MII), global information infrastructure (GII), etc.].

The models also require different resolution when used at the spectrum, levels. This resolution difference is a result of the requirements and the unique situations or problems at each of the levels.

For example, at the platform level the content of the message traveling within the platform is very important, as is the knowledge of whether the entire message reached its intended destination in a timely manner. The threat effects occur primarily at the platform or node level; the communication links between platforms or nodes are the other target of the threats. The types of questions being resolved at the platform level include whether the platform is reporting its correct position in the situational awareness messages that it is sending out, does the TOC send a call for fire to the correct unit, etc. Resolving these types of questions requires knowledge of messages content.

At the networked platform and system-of-system levels of the spectrum the content of the messages is much less important, as the content is only utilized at the platform or node level of

the spectrum. The types of metrics being determined at these higher spectrum levels are quantities such as message completion rate and bit error rate.

Transferring model results between spectrum levels becomes an area demanding detailed concern. If information is passed up to the networked platform level from the platform level, the questions addressed must be considered before the data is modified. It should be noted that this passing, or mapping, of information between spectrum levels is often a nonlinear process due to the networking architectures. To answer certain questions, (e.g., what is the impact from a platform incorrectly reporting its position in situational awareness messages?) the content of messages must remain intact. As specific information, such as platform position is passed up through the modeling spectrum to determine information such as how and where it is distributed, the information must then be passed back down to the platform level to determine what impact the content has on a receiving platform or node. An example of a case where content is not important or needed may be the investigation of the required bandwidth of a communications connection. Here, the questions addressed are those such as: What is the message completion rate? What is the message throughput time? Answer: the information contained in the messages (or content) has no bearing, and retaining this information may actually slow down the simulation. By discarding or not even producing content, the questions can be resolved to the desired level of detail.

The information flow modeling approach has the potential of being of great benefit to the platform/node developers. One of these benefits is in the area of testing contemplated modifications to system software before actually programming the intended change. The functionality of the contemplated change can be put into the information flow modeling to determine if the results are what are intended or whether additional problems result from the contemplated change. This approach will not only save the platform/node developers' programmer time, it will also reduce the time demands of resources such as system integration laboratories (SILs), which are used to ensure that the actual platform or node functions correctly and reliability.

This IOVSA process will contribute to the DITSCAP process activities under phases I, II, and III. Modeling and simulation present several advantages for vulnerability and survivability assessment work. It is nondestructive, usually cost effective, and flexible enough to accommodate new "real world" data. It is also ideal for predicting susceptibilities and vulnerabilities in the composite environment found on Defense Department systems, support systems, and their components involved in battlefield operations.

5.4 Experimental Vulnerability Assessment Process. This portion of the IOVSA process consists of an actual field or laboratory IO experiment to either confirm or negate the predicted results from the analytical vulnerability assessment.

Experiments typically involve a thorough examination of the system configuration, automated and manual assessment of susceptibilities and vulnerabilities identified in previous IOVSA processes, and a reliability analysis of operating system and application software. Also, susceptibilities introduced by application programs are assessed and analyzed in the process.

The purpose of a laboratory or field IO experiment would be to:

(a) identify potential operating system susceptibilities and vulnerabilities (system configuration, application software, network connectivity, etc);

(b) evaluate the effectiveness of Army C2 Protect tools;

(c) determine survivability of the weapons systems' platform under specific denial-of-service attacks; and

(d) provide protection assessment with recommendations on those information warfare threats that impact survivability.

Typically during a laboratory or field IO experiment, the following functional layers of IT components are investigated at both the item and platform levels:

(a) users, operators, and administrators,

(b) application software,

(c) middleware,

(1) data base management systems (DBMS),

(2) data communication equipment (DCE), etc…,

(d) networking,

(e) operating systems, and

(f) hardware.

An annotated IOVSA experimental test plan template is in the Appendix.

6. Protection Assessment and Recommendations

6.1 Introduction. The objective of this phase is to formally assess susceptibilities and vulnerabilities of a system with risk management procedures, and then to propose recommendations for the control, elimination, and/or mitigation of those susceptibilities and vulnerabilities. SLAD maintains a laboratory to test the most recent protection mechanisms from both commercial and research institutions. Research and development to extend and modify products to suit customer needs is also part of the work performed in the survivability laboratory. SLAD's goal is to enhance the overall survivability of the system.

In general, this IOVSA phase assists in completing DITSCAP phase III requirements.

6.2 Process Activities: Protection Assessment and Recommendation Criteria. DOD and the U.S. Army have established specific information assurance (IA) criteria that are mandatory for IO vulnerability and survivability assessments of IT system. Those criteria include:

(a) availability,

(b) confidentiality,

(c) identification,

(d) integrity, and

(e) nonrepudiation.

The above criteria require that systems have certain properties which demonstrate an ability to maintain minimum essential system requirements for the completion of a mission and ultimately survivability. The IOVSA process investigates these properties described in the Glossary.

6.3 Sample Assessment Recommendations. IOVSA recommendations will fall into three categories: (1) elimination of a susceptibility or vulnerability; (2) mitigation of a vulnerability without elimination of the susceptibility; and (3) reduction of a susceptibility or vulnerability with a risk management evaluation of any residual risk.

The first category of recommendations might involve a suggestion to eliminate host services or to reconfigure an application. For example, the Unix operating system (OS) out-of-the-box typically activates many default services in the "/etc/inetd.conf" file. A PEO/PM, who has

chosen Unix as the baseline OS, may be unaware of the consequences in accepting default services. Two services in particular, echo and chargen, are rarely necessary for the operation of an IT system, but both have known vulnerabilities to denial-of-service exploit program attacks. SLAD analysts would recommend the elimination of the services to preclude any disruption to the system or any interference in its mission accomplishment. Similarly, the SendMail application has wide use throughout DOD to provide mail service. The program's default configuration may permit an attacker to determine who has a mail account on the server and the account name. This information could facilitate a brute-force password guessing attack against the server. SLAD analysts would recommend a reconfiguration of the application to eliminate this flow of information.

The second category of recommendations might involve a suggestion to mitigate known OS and application program vulnerabilities, or to configure an application for secure operations. For example, SUN Microsystems issues numerous advisories identifying known vulnerabilities in its Solaris OS and suggests either manual fixes or software patches to address specific problems. While a PEO/PM may implement procedures to incorporate these vendor suggestions into a formal software upgrade program, flaws in the implementation may result in the failure to install essential patches, or in the improper configuration of the patch. During an experimental test, SLAD analysts would determine the specific OS configuration of the system and compare it against the suggested vendor configuration. Analysts would then execute program attacks to verify either the success of the patch to mitigate vulnerabilities, or the impact on the system's mission performance and survivability in cases where the PEO/PM had not installed a patch. Similarly, the file transfer protocol (FTP) application is generally an essential application which has unfortunately experienced several significant vulnerability exposures. SLAD analysts would examine the configuration of the application and determine if there are known configuration errors or omissions that would permit a successful attack on the system. The intent would be to ensure that the application's configuration is both functional to mission requirements and as secure as possible to enhance survivability. Since new OS and application program vulnerabilities may appear in the future, recommendations in this category will seek to mitigate

known vulnerabilities; but obviously, the susceptibility inherent within any OS or critical application cannot be eliminated.

The third and final category of recommendations might involve a suggestion to reconfigure an OS or application to control a known susceptibility or vulnerability, but with no expectation to eliminate either condition. For example, there are many denial-of-service attacks, such as the ping of death and synchronization (SYN) flooding, which exploit host and network services. These services are essential for operating a system and cannot be eliminated. Additionally, vendors and software developers may be unable to issue patches which positively mitigate known exploit program attacks against the services. However, there may exist configuration criteria which will allow a PEO/PM to control the impact and severity of the attack on a system's mission performance. SLAD analysts would examine such services, execute actual exploit program attacks, and analyze the results. Recommendations might include adopting more robust vendor configuration controls, utilizing a packet-filtering firewall, or both. The intent would be to present the PEO/PM with the necessary information to make an informed risk management decision regarding the overall survivability of a system.

7. Summary

The IOVSA process facilitates a focused effort to provide decision makers with the necessary information to make informed decisions concerning the IO susceptibilities and vulnerabilities of their systems. With this information, decision makers can evaluate countermeasures and protection recommendations to enhance of any system's ability to perform its assigned mission.

The IOVSA process establishes a baseline for the assessment of IO effects. In an IO environment, the objective is to protect and defend ones own information, information infrastructure, and information systems, while taking advantage of the enemy's information resources. As discussed in this report, the IOVSA primarily addresses information assurance (IA) of military component level and weapon systems with information technology (IT) items. Through the use of component damage or dysfunction metrics, the IOVSA process is quite

suitable as a means of integrating other threat disciplines. The component damage or dysfunction can either be transient or permanent in nature. The transient class of threats may include information warfare (IW), radio frequency directed energy (RFDE), electronic warfare (EW), electromagnetic environmental effects (E3), atmospherics, and other similar threats. The permanent class of threats may include conventional ballistics, behind-armor debris (BAR), shrapnel, directed energy, and other similar threats. The IOVSA process description will become the blueprint used to incorporate these multiple disciplines into one coherent and integrated IO survivability analysis methodology.

This IOVSA process fulfills the DITSCAP methodology requirements to the extent that any designated approving authority (DAA) can leverage these efforts to satisfy various tasks and steps within each DITSCAP phase, which leads to the certification and accreditation of an IT system.

INTENTIONALLY LEFT BLANK.

8. References

1. Department of Defense. "DOD Information Technology Security Certification and Accreditation Process (DITSCAP)." Department of Defense Instruction Number 5200.40, 30 December 1997.

2. U.S. Army Materiel Command. "Electronic Warfare Vulnerability Assessment (EWVA) Process Description." Joint Logistics Commander's Joint Coordinating Group, Electronic Warfare, Alexandria, VA, 16 June 1994.

3. zum Brunnen, R. L. "The Methodology Process Flow of a SLAD Information Systems Survivability Assessment." ARL-TR-1747, U.S. Army Research Laboratory, Aberdeen Proving Ground, MD, August 1998.

4. U.S. Department of Army. "Information Operations." FM 100-6, August 1996.

5. CORBETT Technologies, Inc. "Draft DOD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Document." 228 North Saint Asaph Street, Alexandria, VA, to be published.

6. DeMarco, T. "Structured Analysis and System Specification." Englewood Cliffs, NJ: Yourdon Press, 1979.

7. Neumann, P. G. "Practical Architectures for Survivable Systems and Networks: Phase-One Final Report." SRI International, 28 January 1999.

INTENTIONALLY LEFT BLANK.

Appendix:

Generic Experimentation Plan for an Information Operations Vulnerability/Survivability Assessment

INTENTIONALLY LEFT BLANK.

The following experimentation plan is generic in nature and is meant to address information technology (IT) items that range from single standalone computers to networked battlefield systems and on to systems-of-systems. This plan will require detailed tailoring for each item or system under investigation depending on its information systems, networks, operating systems, application software, and C-2 Protect software. The final procedures used for the experimentation will be put together in conjunction with the program management office (PMO).

I. PURPOSE. The laboratory-type experimentation on IT items has these purposes: (a) to identify potential operating system susceptibilities and vulnerabilities; (b) to evaluate the effectiveness of Army C-2 Protect software tools as configured on the weapon system to mitigate susceptibilities and vulnerabilities; (c) to determine the survivability of the weapons systems platform under specific denial-of-service attacks; and (d) to provide a protection assessment with recommendations on those Information Warfare threats which impact survivability.

II METHODOLOGY. The methodology for an information operations vulnerability/survivability assessment (IOVSA) includes five phases: system familiarization, system design analysis, threat definition and susceptibility assessment, vulnerability risk and susceptibility assessment, and protection assessment and recommendations.

III. HARDWARE/SOFTWARE/NETWORK REQUIREMENTS. The Survivability/Lethality Analysis Directorate (SLAD) will furnish two government-owned computer platforms. These computing systems will have software installed to conduct the analysis. The weapons systems platform PMO will furnish, or arrange access to the IT items or their software integration laboratory (SIL). (Note: From here forward, the use of "IT items" means whichever is applicable—weapon system platform, software integration laboratory, or both.) The IT items will have all the operating system software, application software, and C-2 Protect software tools specified by the current IT items' configuration management policy. SLAD will require network and direct connectivity to the IT items

and the ability to print files and reports from both supplied computer platforms. Both Ethernet and tactical connections are necessary. A licensed copy of a commercial version of the scanning tool will be used to scan the IT items. Either the PMO's copy, if they have one, or SLAD's copy will be used. This may require that the network IP addresses on the weapon system be reconfigured for this scan. SLAD will provide specific IP addresses if reconfiguration is required. Any routers in the network may require reconfiguration. SLAD will also require a root account and a nonprivileged account on the IT items.

IV. <u>THREAT ASSUMPTIONS.</u> The threat assumptions considered relevant to the experiment need to be documented. Intelligence source documents, especially the system threat assessment report (STAR), should be consulted as a basis for this work. Generalized intelligence estimates may also be applicable. For example, if an IT item will have network connectivity when fielded, the documented threat assumptions should address general IT item vulnerabilities in a networked environment. Unless there is an essential reason for including classified defense information within the test plan, referencing the classified sources is the preferred solution. If the STAR or other validated threat document is referenced, any deliverables should relate experiment results and recommendations to these documents.

When designing the experiments, it may be desirable to include where a validated threat is in appropriate, particularly if the focus is on the identification and potential impact of susceptibilities. An experiment on an operating system or on a specific application illustrates this case. Hypothetical threat descriptions may be substituted during the experiments for verification purposes. Experience shows that during this verification period, a major portion of the vulnerabilities are discovered.

The experiment assumes these levels of threat exist, whether validated or not, for the operating system and platform without regard to any specific mission and/or application program:

Level 1 – A user has network access, but lacks authorization for any access to the system.

Level 2 – A user has network access and authorized access to the system, but intentionally exceeds the authorization.

Level 3 – A user has local physical access to the platform, but lacks authorization for access to the system.

Level 4 – A user has local physical access to the platform and authorized access to the system, but exceeds the authorization.

V. EXPERIMENTAL PROCEDURES.

A. Examine the configuration and installation of the approved software tools from the Army C-2 Protect toolbox and document the results. (Note: Analyzing the configuration should be done before any testing/experimenting is conducted.)

B. Reconfigure the network IP addresses to the required domain, if necessary.

C. Connect the SLAD computer platforms via Ethernet to the IT items' network.

D. Test the network connectivity of the SLAD platforms.

E. Test and verify the hardware and software configuration of the SLAD platforms.

F. Identify and inspect (while logged in as root) all configuration files for the application software, C-2 Protect tools, and operating system on the weapon system; save the results.

G. Identify and inspect (while logged in as root) all configuration files for the operating system and assessment tools on SLAD's assessment computers; save the results.

H. Identify (while logged in as root) all executable files for the application software, C-2 Protect tools, and operating system on the weapon system; save the results.

I. Identify and inspect (while logged in as root) all periodic system processes on the weapon system; save the results.

J. Execute various port scans from the SLAD computers against the IT items; save the results.

K. Analyze and compare the results of the port scans.

L. Execute the applicable network-scanning tool using a heavy scan template against the IT items from SLAD's assessment computers; save the results.

M. Analyze and compare the results of these two scans.

N. Execute additional scans with SLAD modified templates to include one dedicated to denial of service attacks; save the results.

O. Analyze these additional reports and identify susceptibilities and vulnerabilities for further experimentation.

P. Execute specific exploit scripts from SLAD's computers against the weapon system's ports and services; save the results.

Q. Transfer (as a nonprivileged user) exploit scripts/programs from SLAD's computers to the weapon system's computer. Ensure that the exploit scripts/programs reside in a nonprivileged account and are not owned by a privileged user.

R. Execute specific exploit scripts from a nonprivileged account on the IT items; save the results.

S. Analyze the results of the exploit scripts.

T. Connect the SLAD computer platforms via tactical configurations to the IT items' network.

U. Repeat only appropriate procedures from C through S above; save the results.

V. Examine, if appropriate, the security configuration of any network router; document the results.

W. Install the appropriate security evaluation software on the IT items; save the results.

X. Test the effectiveness of installed antiviral software to detect live samples of malicious software either through electronic transmission via mail or file transfer protocol (FTP), or from the mounting of media with infected files.

Note: It is only during procedures W and X that additional software is actually introduced into the IT items.

Y. During a period in the experimentation process, hypothetical threat descriptions are investigated for verification purposes. During this verification period, a major portion of the vulnerabilities are discovered.

VI. DELIVERABLES. SLAD will analyze all data collected and provide a written assessment as to the survivability of the IT item under a simulated IW attack. Where applicable, the assessment will provide recommendations to improve survivability.

Glossary

Ability to Maintain Minimum Essential System Requirements	The system's ability to conduct operations in the presence of unforeseen adverse conditions. This also involves establishing minimum operating requirements. The user of the system generates these requirements based on the minimum system functionality needed to complete mission requirements.
Accountability	Property that allows auditing of IT system activities to be traced to persons or processes that may be then held responsible for their actions. Accountability includes authenticity and nonrepudiation.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator; or, a means of verifying an individual's authorization to receive specific categories of information.
Authenticity	The property that allows the ability to validate the claimed identity of a system entity.
Authorization and Accountability of Systems and Users	A system's capability to control which subsystems and individuals are using it. Otherwise, it may be vulnerable to spoofing attacks, penetrations, and other forms of misuse. After any such attack, the system's inability to provide real-time (or at least rapid) accountability and audit-trail analysis may lead to additional compromises of survivability.
Availability	Timely, reliable access to data and information services for authorized users.
Confidentiality	Assurance that information is not disclosed to unauthorized persons, processes, or devices.
Data Availability	The system's ability to prevent disruption in timely access to data, including sensor data in a control system. Multiple versions of critical data and alternative sensors can help increase data availability.
Data Confidentiality	The system's ability to prevent undesired data disclosure. For example, a penetrator could obtain sensitive data that would compromise the application's ability to fulfill its requirements.

Data Integrity	The attribute of data that is related to the preservation of its meaning and completeness, the consistency of its representation(s), and its correspondence to what it represents.
Fault Tolerance	The system's ability to prevent undesired effects resulting from failure of underlying hardware components, subsystems, or the entire system. Essentially, fault tolerance is both a system integrity issue and a system reliability issue. Constructive use of redundancy is essential. Survivability is a particular concern when the nominal fault tolerance coverage is expected.
Functional Correctness	Assurance that a flaw in the application or in the computer operating system, or a human error in system maintenance, cannot compromise the application. Good software engineering, development practices, and system operation are important, but are clearly not enough by themselves.
Functional Timeliness	Can include strict bounds in hard-real-time systems or best effort intentions in fuzzy-real-time systems.
Information System	Any telecommunication or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware.
Information Technology	The hardware, firmware, and software used as part of the information system to perform DOD information functions. This definition includes computers, telecommunications, automated information systems, and automatic data processing equipment. IT includes any assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.
Infrastructure-Centric	A security management approach that considers information systems and their computing environment as a single entity.
Nonrepudiation	Assurance that the sender of data is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so neither can later deny having processed the data.
Real-Time Accountability	Can include anomaly detection and audit-trail analysis.

Real-Time Availability
Assurance that the real-time processing can be done in a timely way and that the system is protected against maliciously or accidentally caused delays. This property includes the real-time availability of the system, data, and other resources.

Risk
A combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will have an adverse impact, and the severity of the resulting impact.

Risk Assessment
The process of analyzing threats to and vulnerabilities of an IT system; the potential impact that the loss of information or capabilities of a system would have on national security. The resulting analysis is used as a basis for identifying appropriate and effective measures.

Risk Management
Process concerned with the identification, measurement, control, and minimization of security risks in IT systems to a level commensurate with the value of the assets protected.

Survivability
Survivability is the ability of a computer communication system-based application to satisfy and to continue to satisfy certain critical requirements (e.g., specific requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions.*

Susceptibility
Technical characteristics describing inherent limitations of a system that have potential for exploitation by the enemy.

System
A set of interrelated components consisting of mission, environment, and architecture as a whole.

System Availability
The system's ability to prevent system and communication outages, including temporary unavailability of resources. Such outages may include malicious or accidental denials of system service.

System Confidentiality
The system's ability to prevent the undesired dissemination or acquisition of sensitive system code or data, particularly if the application can be compromised. Otherwise, for example, knowledge of the system design, a specific algorithm, a piece of code, a password, a cryptographic key, a network authenticator, or a piece of equipment could lead to a system subversion.

* Neumann, P. G. "Practical Architectures for Survivable Systems and Networks: Phase-One Final Report." *SRI International*, 28 January 1999.

System Entity	A system subject (user or process) or object.
System Integrity	Quality of an IT system to perform its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
TEMPEST	Short name referring to investigation, study, and control of compromising emanations from IT equipment.
Threat	Any circumstance or event with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
Threat Assessment	A formal description and evaluation of a threat to an IT system.
Timely Detection and Correction of Deviant System Behavior	The system's ability to reconfigure itself in the face of nontolerated faults or penetrations. Recovery from serious outages may or may not be allowed to incur long time delays or human intervention. In cases where human intervention is not possible, thorough advanced planning is necessary.
User	Person or process authorized to access an IT system.
Vulnerability	Weakness in an information system, cryptographic system, or components (e.g., system security procedures, hardware design, internal controls) that could be exploited.
Vulnerability Assessment	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

NO. OF COPIES	ORGANIZATION
2	DEFENSE TECHNICAL INFORMATION CENTER DTIC DDA 8725 JOHN J KINGMAN RD STE 0944 FT BELVOIR VA 22060-6218
1	HQDA DAMO FDT 400 ARMY PENTAGON WASHINGTON DC 20310-0460
1	OSD OUSD(A&T)/ODDDR&E(R) R J TREW THE PENTAGON WASHINGTON DC 20301-7100
1	DPTY CG FOR RDA US ARMY MATERIEL CMD AMCRDA 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001
1	INST FOR ADVNCD TCHNLGY THE UNIV OF TEXAS AT AUSTIN PO BOX 202797 AUSTIN TX 78720-2797
1	DARPA B KASPAR 3701 N FAIRFAX DR ARLINGTON VA 22203-1714
1	NAVAL SURFACE WARFARE CTR CODE B07 J PENNELLA 17320 DAHLGREN RD BLDG 1470 RM 1101 DAHLGREN VA 22448-5100
1	US MILITARY ACADEMY MATH SCI CTR OF EXCELLENCE DEPT OF MATHEMATICAL SCI MADN MATH THAYER HALL WEST POINT NY 10996-1786

NO. OF COPIES	ORGANIZATION
1	DIRECTOR US ARMY RESEARCH LAB AMSRL D D R SMITH 2800 POWDER MILL RD ADELPHI MD 20783-1197
1	DIRECTOR US ARMY RESEARCH LAB AMSRL DD 2800 POWDER MILL RD ADELPHI MD 20783-1197
1	DIRECTOR US ARMY RESEARCH LAB AMSRL CS AS (RECORDS MGMT) 2800 POWDER MILL RD ADELPHI MD 20783-1145
3	DIRECTOR US ARMY RESEARCH LAB AMSRL CI LL 2800 POWDER MILL RD ADELPHI MD 20783-1145

ABERDEEN PROVING GROUND

NO. OF COPIES	ORGANIZATION
4	DIR USARL AMSRL CI LP (BLDG 305)

NO. OF COPIES	ORGANIZATION
1	OASD C3I MR BUCHHEISTER RM 3D174 6000 DEFENSE PENTAGON WASHINGTON DC 20310-6000
1	OUSD AT STRT TAC SYS DR SCHNEITER RM 3E130 3090 DEFENSE PENTAGON WASHINGTON DC 20310-3090
1	OUSD AT S&T AIR WARFARE RM 3E139 R MUTZELBUG 3090 DEFENSE PENTAGON WASHINGTON DC 20301-3090
1	OUSD AT S&T LAND WARFARE RM EB1060 A VIILU 3090 DEFENSE PENTAGON WASHINGTON DC 20310-3090
1	UNDER SEC OF THE ARMY DUSA OR ROOM 2E660 102 ARMY PENTAGON WASHINGTON DC 20310-0102
1	ASST SECY ARMY ACQUISITION LOGISTICS TCHNLGY SARD ZD ROOM 2E673 103 ARMY PENTAGON WASHINGTON DC 20310-0103
1	ASST SECY ARMY ACQUISITION LOGISTICS TCHNLGY SARD ZP ROOM 2E661 103 ARMY PENTAGON WASHINGTON DC 20310-0103
1	ASST SECY ARMY ACQUISITION LOGISTICS TCHNLGY SAAL ZS ROOM 3E448 103 ARMY PENTAGON WASHINGTON DC 20310-0103

NO. OF COPIES	ORGANIZATION
1	OADCSOPS FORCE DEV DIR DAMO FDZ ROOM 3A522 460 ARMY PENTAGON WASHINGTON DC 20310-0460
1	HQDA ODCSPER DAPE MR RM 2C733 300 ARMY PENTAGON WASHINGTON DC 20310-0300
1	US ARMY MATERIEL CMD DEP CHF OF STAFF FOR RDA SCIENCE TECH ENG AMCRDA 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001
1	US ARMY MATERIEL CMD DEP CHF OF STAFF FOR RDA SCIENCE TECH ENG AMCRDA T 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001
1	US ARMY ARMAMENT RDEC AMSTA AR TD M FISETTE BLDG 1 PICATINNY ARSENAL NJ 07806-5000
1	US ARMY MISSILE RDEC AMSMI RD W MCCORKLE REDSTONE ARSENAL AL 35898-5240
1	NATICK SOLDIER CENTER SBCN T P BRANDLER KANSAS STREET NATICK MA 01760-5056
1	US ARMY TANK AUTOMTV RDEC AMSTA TR J CHAPIN WARREN MI 48397-5000

NO. OF COPIES	ORGANIZATION
1	US ARMY INFO SYS ENGRG CMD AMSEL IE TD F JENIA FT HUACHUCA AZ 85613-5300
1	US ARMY SIM TRNG INST CMD AMSTI CG M MACEDONIA 12350 RESEARCH PKWY ORLANDO FL 32826-3726
1	US ARMY TRADOC BATTLELAB INTEGRATION TECH B CONCEPTS DIR ATCD B FT MONROE VA 23561-5000
1	ARMY TRADOC ANL CTR ATRC W MR KEINTZ WSMR NM 88002-5502
2	DEPUTY CHIEF OF STAFF INTELLIGENCE DAMI ZA DAMI IM 2511 JEFFERSON DAVIS HIGHWAY STE 9300 ARLINGTON VA 22202-3910
1	ASSISTANT SECY ARMY ACQUISITIONS LOGISTICS AND TECHNOLOGY SAAL SA DIRECTOR OF AVIATION 103 ARMY PENTAGON WASHINGTON DC 20310-0130
1	DEPUTY CHIEF OF STAFF PERSONNEL DAPE MR 300 ARMY PENTAGON WASHINGTON DC 20310-0300
1	US ARMY TECOM CSTE OP PARK CENTER IV 4501 FORD AVE ALEXANDRIA VA 22302-1458

NO. OF COPIES	ORGANIZATION
5	DIRECTOR INFORMATION SYSTEMS FOR COMMAND CONTROL COMMO & COMPUTERS SAIS IAS 2511 JEFFERSON DAVIS HWY STE 11800 ARLINGTON VA 22202
13	DEPUTY CHIEF OF STAFF OPERATIONS & PLANS DAMO ADO DAMO TR DAMO ZD DAMO FDJ DAMO FDB DAMO FDC DAMO FDD DAMO FDE AD DAMO FDF DAMO FDG FA DAMO FDW DAMO ODL DAMO ODP 400 ARMY PENTAGON WASHINGTON DC 20310-0400
1	COMMANDER US ARMY ELECTRONIC PROVING GROUND S2 FT HUACHUCA AZ 85613
1	DEPARTMENT OF THE ARMY PROGRAM EXECUTIVE OFFICER AIR & MISSILE DEFENSE 215 WYNN DRIVE STE 201 HUNTSVILLE AL 35807-3801
1	DEPARTMENT OF THE ARMY PROGRAM EXECUTIVE OFFICER AVIATION SFAE AV BUILDING 5300 REDSTONE ARSENAL AL 35898-5000

NO. OF COPIES	ORGANIZATION
1	DEPARTMENT OF THE ARMY PROGRAM EXECUTIVE OFFICER COMMAND CONTROL & COMMUNICATIONS SYSTEMS SFAE C3S FT MONMOUTH NJ 07703-5501
1	DEPARTMENT OF THE ARMY PROGRAM EXECUTIVE OFFICER GROUND CBT SPT SYSTEM SFAE GCSS W WARREN MI 48397-5000
1	DEPARTMENT OF THE ARMY PROGRAM EXECUTIVE OFFICER INTELLIGENCE ELECTRONIC WARFARE & SENSORS SFAE IEWS FT MONMOUTH NJ 07703-5501
1	DEPARTMENT OF THE ARMY PROGRAM EXECUTIVE OFFICER STANDARD ARMY MANAGEMENT INFORMATION SYSTEMS SFAE PS 9350 HALL ROAD STE 142 FT BELVOIR VA 22060-5526
1	DEPARTMENT OF THE ARMY PROGRAM EXECUTIVE OFFICER TACTICAL MISSILE SFAW MSL REDSTONE ARSENAL AL 35898-8000
1	DEPARTMENT OF THE ARMY INFORMATION WARFARE PRODUCT MANAGER 7484 CANDLEWOOD ROAD STE M L HANOVER MD 21076
1	US ARMY MATERIEL COMMAND AMCRDA AI TILO 5001 EISENHOWER AVE ALEXANDRIA VA 22333-0001

NO. OF COPIES	ORGANIZATION
1	COMMANDER US ARMY AVIATION AND MISSILE COMMAND AMSMI REDSTONE ARSENAL AL 35898-5160
1	COMMANDER US ARMY COMMUNICATIONS ELECTRONICS COMMAND AMSEL AC FT MONMOUTH NJ 07703-5000
1	US ARMY TACOM AMSTA DSA WARREN MI 48397-5000
3	COMMANDER FORSCOM AFIN SD AFOP OC AFIX CCP FT MCPHERSON GA 30330-1062
1	COMANDER US ARMY SIGNAL COMMAND AFSC PLM FT HUACHUCA AZ 85613-5000
1	COMMANDER US TOTAL ARMY PERSONNEL COMMAND TAPC ZA 200 STOVALL STREET ALEXANDRIA VA 22332-400
2	COMMANDER US ARMY CAC & FT LEAVENWORTH ATZL CG ATZL TP 415 SHERMAN AVE FT LEAVENWORTH KS 66027-2300
1	US ARMY CASCOM ATCL-K 2521 E AVE FT LEE VA 23801-1701

NO. OF COPIES	ORGANIZATION
20	COMMANDER US ARMY TRADOC ATCD B ATCD BP ATCD FM ATCD G ATCD GI ATCD J ATCD Q ATCD RO ATCD S ATDO A ATDO I ATDO ZA ATIM F ATIM I ATIN ZA ATIN I ATIN NSA ATAN SM ATBO S ATTG ZA FT MONROE VA 23651-5000
3	NORAD USSPACECOM/J6O CHIEF C4 SYSTEMS OPERATIONS DIVISION COL J RADER 250 S PETERSON BLVD STE 116 PETERSON AFB CO 80914-3050
4	US ARMY CASCOM & FT LEE ATZM CG ATZM CS ATCL CM ATCL CT TSM 3901 A AVE FT LEE VA 23801-1809
2	US ARMY TRADOC ANALYSIS CENTER ATRC TD ATRC RM 255 SEDGWICK AVE FT LEAVENWORTH KS 66027-2345

NO. OF COPIES	ORGANIZATION
1	US ARMY TRADOC ANALYSIS CENTER WHITE SANDS MISSILE RANGE ATRC WGA WHITE SANDS MISSILE RRANGE NM 88002-5502
3	US ARMY TRAINING SUPPORT CENTER ATIC DM ATIM TIS ATIC CTC FT EUSTIS VA 23604-5166
2	NATIONAL SIMULATION CENTER ATZL NCS P 410 KEARNEY AVE FT LEAVENWORTH KS 66027-1306
2	COMMANDER USAADACENFB ATZC CG ATZC CD 1733 PLEASTON ROAD FT BLISS TX 79916-6816
3	US ARMY ARMOR CTR & FT KNOX ATZK CG ATZK TS ATZK XXI FT KNOX KY 40121-5000
1	US ARMY FIELD ARTILLERY CTR & FT SILL ATZR CG FT SILL OK 73503-5000
2	US ARMY AVIATION CTR & FT RUCKER ATZQ CG ATZQ CD FT RUCKER AL 36362-5000
1	US ARMY AVIATION CTR & FT RUCKER ATZQ TSM C FT RUCKER AL 36362-5010

NO. OF COPIES	ORGANIZATION
1	US ARMY AVIATION CENTER & FT RUCKER ATZQ TSM LB FT RUCKER AL 36362-5012
2	US ARMY ENGINEER CENTER & FT LEONARD WOOD ATZT CG ATZT CD FT LEONARD WOOD MO 65473-5000
4	US ARMY INFANTRY CENTER & FT BENNING ATZB CD ATZB FS ATZB BV ATZB TS FT BENNING GA 31905-5000
6	US ARMY INTELLIGENCE CTR & FT HUACHUCA ATZS CG ATZS CD ATZS CDA ATZS JS ATZS CDU ATZS CDG FT HUACHUCA AZ 85613-6000
1	US ARMY QUARTERMASTER CENTER & FT LEE ATSM CD 1201 22D ST FT LEE VA 23801-1601
3	US ARMY SIGNAL CENTER & FT GORDON ATZH NM ATZH TR ATZH TS FT GORDON GA 30905-5310
2	US ARMY TRANSPORTATION CENTER & FT EUSTIS ATZF CD ATZF TW FT EUSTIS VA 23604-5000

NO. OF COPIES	ORGANIZATION
2	III CORPS & FT HOOD AFZF GS AFZF DFCC FT HOOD TX 76544-5000
1	XVIII CORPS & FT BRAGG G2 FT BRAGG NC 28307-5000
1	704TH MILTY INTELLIGENCE BRIGADE S3 FT MEADE MD 20755
2	902ND MILITARY INTELLIGENCE GROUP IAGPA BIWB IAGPA C ACIC FT MEADE MD 20755
1	DIRECTOR CENTRAL INTELLIGENCE AGENCY OSWR PO BOX 1925 WASHINGTON DC 20013
1	DIRECTOR OPERATIONAL PLANS & INTEROPERABILITY J7 7000 JOINT STAFF PENTAGON WASHINGTON DC 20318-7000
3	DIRECTOR DEFENSE INFORMATION SYSTEM AGENCY D3 D25 D314 7010 DEFENSE PENTAGON WASHINGTON DC 20301-7010
1	US ARMY ARDEC JOINT MILITARY LIAISON OFC ATFE LO AC BLDG 1 DOVER DE 07801-5001

NO. OF COPIES	ORGANIZATION
1	JOINT C4ISR BATTLE CENTER IO IA 116 LAKEVIEW PARKWAY STE 150 SUFOLK VA 23435-2697
1	NATIONAL GROUND INTELLIGENCE CTR IANG SSC 220 SEVENTH STREET NE CHARLOTTESVILLE VA 22902-5396
3	COMMANDER IN CHIEF US SPECIAL OPERATIONS COMMAND J3 J6 J7 7701 TAMPA POINT BLVD MACDILL AIR FORCE BASE FL 33621-5323
1	US ARMY RESEARCH LAB AMSRL SL PLANS & PGMS MGR WSMR NM 88002-5513
1	US ARMY RESEARCH LAB AMSRL SL E WSMR NM 88002-5513
30	US ARMY RESEARCH LAB AMSRL SL EA D LANDIN WSMR NM 88002-5513
10	US ARMY RESEARCH LAB AMSRL SL EA C MCDONALD WSMR NM 88002-5513
10	US ARMY RESEARCH LAB AMSRL SL EI A BARNES FT MONMOUTH NJ 07703-5602

NO. OF COPIES	ORGANIZATION
24	US ARMY RESEARCH LAB AMSRL SL EA R FLORES J SMITH J LAROW S CUNICO K NIX R ORTEGA C OCHOA N CHRISTIANSON E GUNDERSON T MCDONALD R FRENCH I LUJAN D WILLIAMS K MORRISON G MAREZ L ESCUDERO G ANAYA P DJANG B FARRAN R GONZALEZ G GUZIE F MOORE T READER L SWEARINGEN WHITE SANDS MISSILE RANGE NM 88002-5513
11	US ARMY RESEARCH LAB AMSRL SL EM J PALOMO E ZARRET O PAYAN R HERNANDEZ L ESCUDERO O DAVENPORT C MARAGOUDAKIS G BELL A MARES T MAXWELL J THOMPSON WHITE SANDS MISSILE RANGE NM 88002-5513

NO. OF COPIES	ORGANIZATION
9	US ARMY RESEARCH LAB AMSRL SL EI J NOWAK P BOTHNER C MEINCKE D AMARAL N JERSCHKOW J LIRSKI J LUMA M MASCIULLI W NORCZYK FT MONMOUTH NJ 07703-5602
26	US ARMY EVALUATION CENTER CSTE AEC DR STRILIEN CSTE AEC ADE D WOLF S MOORE CSTE AEC ADE S L THOMSON W WILLIFORD M MORRISSEY S KANG J MITCHELL CSTE AEC ADE C M BAHR H JACKSON B FRASER D BRAWLEY K WU M WOLCHAK R CREVECOEUR J BELL M GREEN CSTE AEC AV J PAGE CSTE AEC AV R REDMOND CSTE AEC AV B S KNAPP CSTE AEC AV B J BURKE D HABEL CSTE AEC AV C C CHU D MESHESHA W PARKER R WATERS 4501 FORD AVE ALEXANDRIA VA 22302-1458

NO. OF COPIES	ORGANIZATION
40	US ARMY EVALUATION CENTER CSTE AEC AV C M GULLEY R JOVEL A MRAZ S NAIR CSTE AEC CCE M MORAN J COX CSTE AEC CCE I S OLIVER C DELUCA J BUTLER D BRITTON T JONES D MUSSER CSTE AEC CCE R J BYNRNE G MCGUIRE L GILL T SCHMIDT CSTE OEC CCE A R TEEL D BURCH W HILL S HUTCHISON B MCVEIGH S TUFTS C MARTIN G PAYNE A TICHENOR S WATKINS PEAY CSTE AEC CSE W BRANCH H ROMBERG CSTE AEC CSE CB M CHIPMAN C SIGLER C BARRETT L HUNTER L JOHNSON D SIMMONS C HOLMAN S TUCKER CSTE AEC CSE CSS B BLAKE J REID S SANDERS J WALKER 4501 FORD AVE ALEXANDRIA VA 22302-1458

NO. OF COPIES	ORGANIZATION
39	US ARMY EVALUATION CENTER CSTE AEC CSE CSS M STEIGERWALD W PATTERSON F SMITH S TUCKER I LEE J LONG R RIDDICK L HADJIOSIF M SYKES D COOK J BELLIZAN CSTE ACE C3E B BARNES I SHEVER CSTE ACE C3E CS C BROWN W KNIGHT J CONEY L DAVIS P SUL M RAHMAN R FLEMONS M VENTERS G SANDERS CSTE ACE C3E CC S BRISTOW R BOYD R HARRIS G GARFINKEL T MALONEY K ASKIN R PACE P VERNER CSTE AEC FSE J ROONEY CSTE AEC FSE R T LIPTAK J MERCER B RAMSEY M LUKER D WASHINGTON CSTE AEC FSE C E MUSKOPF CSTE AEC FSE C3 M JOHNSON J LEWIS 4501 FORD AVE ALEXANDRIA VA 22302-1458

NO. OF COPIES	ORGANIZATION
21	US ARMY EVALUATION CENTER CSTE AEC FSE C3 A MAZYCK W JONES O JOHNSON P CRISE CSTE AEC FSE IED J BROWN H LIGHT CSTE AEC FSE IED A C DEVLIN J GLAZE R THOMAS S STARRUNNER CSTE AEC FSE IED G M WHITAKER C CONNER M LOEW R YI S MINNE R OWEN M FICHTEN P WALTER K THORNTON K WYANT M DOUDZAI PARK CIRCLE IV 4501 FORD AVE ALEXANDRIA VA 22302-1458
4	US ARMY EVALUATION CENTER CSTE AEC SVE S J MINJARES J REZA P THOMPSON R VALASQUEZ FT BLISS TX 79916
1	US ARMY EVALUATION CENTER CSTE AEC SVE S P MOREL FT MONMOUTH NJ 07703-5602

NO. OF COPIES	ORGANIZATION
	ABERDEEN PROVING GROUND
1	SBCCOM RDEC AMSSB RTD J ZARZYCKI 5183 BLACKHAWK RD APG MD 21010-5424
1	US ARMY MATERIEL SYSTEMS ANALYSIS ACTIVITY AMXSY G APG MD 21005-5071
1	US ARMY OC&S ATSL CG APG MD 21005-5201
1	US ARMY DEV TEST COM CSTE DTC TT T APG MD 21005-5055
23	US ARMY EVALUATION CENTER CSTE AEC W HUGHES CSTE AEC ADE T R BOWEN R WEAVER J YOUNGBLOOD N DOMBECK E CUNNINGHAM S FROST D EIMER CSTE AEC AV A R MIRABELLE M ALLEN J PETERS P REICH J TRAN K UNRUH J BURKE C ROSS CSTE AEC CCE W F GASIOROWSKI L BOWMAN R CAMMARATA M CROSS K FENDICK E GRADY H JERKINS 4120 SUSQUEHANNA AVE APG MD 21005-3013

NO. OF COPIES	ORGANIZATION
	ABERDEEN PROVING GROUND (CONT)
38	US ARMY EVALUATION CENTER CSTE AEC CCE W J MEIROSE T MODICA CSTE AEC CSE CS G WINSLOW B STOLARZ P BROWN M DILLION C LEE M PRATHER J ROUSE S TACKETT G BERAN T FRAZIER J STEVENS J VALENTINE CSTE AEC C3E E H BETZ M ALVAREZ W EDLER R FARRELL W HOAFAT A LOPOLITO M PFOUTZ M PLISCOF B QUAGLIA M VINCENT K YU CSTE AEC FSE C B BRAMWELL W CLOWES A SMITH H CHEEVER V BAXIVANOS E PETERS CSTE AEC ILS F PLAYER CSTE AEC ILS A C KARWOWSKI CSTE AEC SV E D DELATTRE CSTE AEC SV E S R POLMADEI T FLORY L HANNAH J MYERS 4120 SUSQUEHANNA AVE APG MD 21005-3013

NO. OF COPIES	ORGANIZATION
	ABERDEEN PROVING GROUND (CONT)
13	US ARMY EVALUATION CENTER CSTE AEC SV E S D SMOOT W SWIDERSKI CSTE AEC SV E L R LAUGHMAN L FILLINGER L KRAVITZ LUKENS POLYANSKI SCOTT T FISHER CSTE AEC RAM S YUHAS C RAYNOR CSTE AEC RAM G R DALTON CSTE AEC RAM A R ANDRULIS 4120 SUSQUEHANNA AVE APG MD 21005-3013
4	US ARMY RESEARCH LAB AMSRL SL BN D FARENWALD B SMITH B RUTH R PARSONS APG MD 21010-5423
2	US ARMY RESEARCH LAB AMSRL SL DR WADE J BEILFUSS
4	US ARMY RESEARCH LAB AMSRL SL B MS SMITH J FRANZ M VOGEL W WINNER
4	US ARMY RESEARCH LAB AMSRL SL BA M RITONDO S JUARASCIO R HENRY J SHORT

NO. OF COPIES	ORGANIZATION
	ABERDEEN PROVING GROUND (CONT)
2	US ARMY RESEARCH LAB AMSRL SL BD J MORRISSEY D LINDELL
8	US ARMY RESEARCH LAB AMSRL SL BE D BELY P KUSS J LIU G KUCINSKI R WEISS S TRENTANELLI R ZIGLER R SANDMEYER
3	US ARMY RESEARCH LAB AMSRL SL BG A YOUNG J PLOSKONKA R GANGLER
1	US ARMY RESEARCH LAB AMSRL SL E M STARKS
6	US ARMY RESEARCH LAB AMSRL SL EA D BAYLOR A BEVEC D ORLANDO D LEADORE D BASSETT R MURK
30	US ARMY RESEARCH LAB AMSRL SL EA R ZUM BRUNNEN
4	US ARMY RESEARCH LAB AMSRL SL EM J FEENEY J ANDRESE C GARRETT J NEALON
1	US ARMY RESEARCH LAB AMSRL SL EC E PANUSKA

INTENTIONALLY LEFT BLANK.

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 2000	Final, Jun - Aug 99

4. TITLE AND SUBTITLE
Information Operations Vulnerability/Survivability Assessment (IOVSA): Process Structure

5. FUNDING NUMBERS
OLE120

6. AUTHOR(S)
Richard L. zum Brunnen, Christopher D. McDonald, Paul R. Stay, Michael W. Starks, and Anthony L. Barnes

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: AMSRL-SL-EA
Aberdeen Proving Ground, MD 21010-5423

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-2250

9. SPONSORING/MONITORING AGENCY NAMES(S) AND ADDRESS(ES)

10.SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

The Survivability/Lethality Directorate (SLAD) of the U.S. Army Research Laboratory (ARL) has developed an information operations vulnerability/survivability assessment (IOVSA) process. The objective of the IOVSA process is to establish a systematic approach that permits analysis and evaluation of the survivability of military component level and weapon systems that include information technology (IT) items. The process will apply throughout the life cycle phases of any Department of Defense (DOD) system that collects, stores, transmits, or processes classified and/or sensitive but unclassified (SBU) information, as well as commercial components to DOD systems. The IOVSA process fulfills many of those process activities required by the DOD Information Technology Security Certification and Accreditation Process (DITSCAP) by providing much of the required vulnerability information.

The IOVSA plan for a particular system is a focused plan that has been designed to provide the decision-makers with the necessary information to make informed decisions concerning the susceptibilities and vulnerabilities of the system to information operations (IO) threats. By addressing the IO threats, the system will significantly improve its survivability by planning for both avoiding and withstanding potential problems with IO-based threats. This report discusses the IOVSA process in detail.

14. SUBJECT TERMS
information operations, information warfare, information system survivability, vulnerability, susceptability, assessment, risk

15. NUMBER OF PAGES
57

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

INTENTIONALLY LEFT BLANK.

USER EVALUATION SHEET/CHANGE OF ADDRESS

This Laboratory undertakes a continuing effort to improve the quality of the reports it publishes. Your comments/answers to the items/questions below will aid us in our efforts.

1. ARL Report Number/Author ARL-TR-2250 (zum Brunnen) Date of Report June 2000

2. Date Report Received ______

3. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which the report will be used.) ______

4. Specifically, how is the report being used? (Information source, design data, procedure, source of ideas, etc.) ______

5. Has the information in this report led to any quantitative savings as far as man-hours or dollars saved, operating costs avoided, or efficiencies achieved, etc? If so, please elaborate. ______

6. General Comments. What do you think should be changed to improve future reports? (Indicate changes to organization, technical content, format, etc.) ______

CURRENT ADDRESS

Organization ______

Name ______ E-mail Name ______

Street or P.O. Box No. ______

City, State, Zip Code ______

7. If indicating a Change of Address or Address Correction, please provide the Current or Correct address above and the Old or Incorrect address below.

OLD ADDRESS

Organization ______

Name ______

Street or P.O. Box No. ______

City, State, Zip Code ______

(Remove this sheet, fold as indicated, tape closed, and mail.)

(DO NOT STAPLE)